tenable network security

Nessus Compliance Checks

Auditing System Configurations and Content

September 30, 2015

(Revision 90)

Table of Contents

Introduction 5
- Prerequisites 5
- Nessus and SecurityCenter Customers 5
- Standards and Conventions 5
- Compliance Standards 6
- Configuration Audits, Data Leakage, and Compliance 6
  - What is an audit? 6
  - Audit vs. Vulnerability Scan 7
  - Example Audit Items 7
    - Windows 7
    - Unix 8
    - Cisco 8
    - Huawei 8
    - Palo Alto Firewall 9
    - IBM iSeries 9
    - NetApp Data ONTAP 9
    - Salesforce 10
    - Databases 10
  - Audit Reports 11
- Credentialed Scanning and Privileged Account Use 11
- Technology Required 12
  - Mobile Device Management (MDM) Compliance Nessus Plugin 12
  - Rackspace Compliance Nessus Plugin 12
  - Unix and Windows Configuration Compliance Nessus Plugins 12
  - Unix and Windows Content Compliance Nessus Plugin 12
  - Database Compliance Nessus Plugin 13
  - IBM iSeries Compliance Nessus Plugin 13
  - Cisco Compliance Nessus Plugin 13
  - Juniper Junos Compliance Nessus Plugin 13
  - Huawei Compliance Nessus Plugin 13
  - Palo Alto Compliance Nessus Plugin 14
  - VMware Compliance Nessus Plugin 14
  - Citrix XenServer Compliance Nessus Plugin 14

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

HP ProCurve Compliance Nessus Plugin 14
FireEye Compliance Nessus Plugin 14
Fortigate FortiOS Compliance Nessus Plugin 14
Amazon AWS Compliance Capability 15
Dell Force10 Compliance Nessus Plugin 15
Adtran AOS Compliance Nessus Plugin 15
SonicWALL SonicOS Compliance Nessus Plugin 15
Extreme ExtremeXOS Compliance Nessus Plugin 15
Check Point GAiA Compliance Nessus Plugin 15
Brocade FabricOS Compliance Nessus Plugin 16
NetApp Data ONTAP Compliance Nessus Plugin 16
SCAP Linux and Windows Compliance Checks 16
MongoDB Compliance Nessus Plugin 16
Salesforce Compliance Nessus Plugin 16
BlueCoat ProxySG Compliance Nessus Plugin 16
Red Hat Enterprise Virtualization (RHEV) Compliance Nessus Plugin 17
Audit Policies 17
Helpful Utilities 17
Unix or Windows Nessus Scanners 17
Credentials for Devices to be Audited 17
Using “su”, “sudo”, and “su+sudo” for Audits 18
sudo Example 19
su+sudo Example 19
Important Note Regarding sudo 20
Cisco IOS Example: 21
Converting Windows .inf Files to .audit Files with i2a 22
Obtaining and Installing the Tool 22
Converting the .inf to .audit 22
Analyzing the Conversion 23
Correct .inf Setting Format 23
Converting Unix Configuration Files to .audit Files with c2a 25
Obtaining and Installing the Tool 25
Create a MD5 Audit File 26
Create Audit File Based on One or More Configuration Files 26
Creating a MAP File 27
Other Uses for the c2a Tool 28

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Manual Tweaking of the .audit Files 28
Converting Unix Package Lists to .audit Files with p2a 29
Obtaining and Installing the Tool 29
Usage 29
Create Output File Based on all Installed Packages 30
Create Output File Based on Package List and Send to the Screen 30
Create Audit File Based on a Specified Input File 30
Example Nessus User Interface Usage 31
Obtaining the Compliance Checks 31
Configuring a Scanning Policy 31
Uploading a Custom Audit Policy 34
Offline Configuration Audits 35
Performing a Scan 37
Example Results 37
Example Nessus for Unix Command Line Usage 38
Obtaining the Compliance Checks 38
Using .nessus Files 38
Using .nessusrc Files 39
Performing a Scan 39
Example Results 39
SecurityCenter Usage 40
Obtaining the Compliance Checks 40
Configuring a Scan Policy to Perform a Compliance Audit 40
Managing Credentials 42
Analyzing the Results 43
Additional Resources 45
About Tenable Network Security 46

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Introduction

This document describes how Nessus 5.x can be used to audit the configuration of Unix, Windows, database, SCADA, IBM iSeries, and Cisco systems against a compliance policy as well as search the contents of various systems for sensitive content.

The phrases "Policy Compliance" and "Compliance Checks" are used interchangeably within this document.

SCADA system auditing is possible with Nessus; however this functionality is outside of the scope of this document. Please reference the Tenable SCADA information page here for more information.

Performing a compliance audit is not the same as performing a vulnerability scan, although there can be some overlap. A compliance audit determines if a system is configured in accordance with an established policy. A vulnerability scan determines if the system is open to known vulnerabilities. Readers will learn the types of configuration parameters and sensitive data that can be audited, how to configure Nessus to perform these audits and how Tenable's SecurityCenter can be used to manage and automate this process.

Prerequisites

This document assumes some level of knowledge about the Nessus vulnerability scanner. For more information on how Nessus can be configured to perform local Unix and Windows patch audits, please refer to the paper "Nessus Credentials Checks for Unix and Windows" available at http://www.tenable.com/products/nessus/documentation.

Nessus and SecurityCenter Customers

Users must be subscribed to commercial Nessus or use SecurityCenter to perform the compliance checks described in this paper. Both are available from Tenable Network Security (http://www.tenable.com/). A more detailed list of the technical requirements to perform the audit checks is discussed in the next few chapters.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd
/home/test/
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Compliance Standards

There are many different types of government and financial compliance requirements. It is important to understand that these compliance requirements are minimal baselines that can be interpreted differently depending on the business goals of the organization. Compliance requirements must be mapped with the business goals to ensure that risks are appropriately identified and mitigated. For more information on developing this process, please refer to the Tenable whitepaper "Maximizing ROI on Vulnerability Management".

For example, a business may have a policy that requires all servers with customer personally identifiable information (PII) on them to have logging enabled and minimum password lengths of 10 characters. This policy can help in an organization's efforts to maintain compliance with any number of different regulations.

Common compliance regulations and guides include, but are not limited to:

- BASEL II
- Center for Internet Security Benchmarks (CIS)
- Control Objectives for Information and related Technology (COBIT)
- Defense Information Systems Agency (DISA) STIGs
- Federal Information Security Management Act (FISMA)
- Federal Desktop Core Configuration (FDCC)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO 27002/17799 Security Standards
- Information Technology Information Library (ITIL)
- National Institute of Standards (NIST) configuration guidelines
- National Security Agency (NSA) configuration guidelines
- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley (SOX)
- Site Data Protection (SDP)
- United States Government Configuration Baseline (USGCB)
- Various State Laws (e.g., California's Security Breach Notification Act - SB 1386)

These compliance checks also address real-time monitoring such as performing intrusion detection and access control. For a more in depth look at how Tenable's configuration auditing, vulnerability management, data leakage, log analysis, and network monitoring solutions can assist with the mentioned compliance regulations, please refer to the Tenable whitepaper "Real-Time Compliance Monitoring".

Configuration Audits, Data Leakage, and Compliance

What is an audit?

Nessus can be used to log into Unix and Windows servers, Cisco devices, SCADA systems, IBM iSeries servers, and databases to determine if they have been configured in accordance to the local site security policy. Nessus can also search the entire hard drive of Windows and Unix systems, for unauthorized content.

It is important that organizations establish a site security policy before performing an audit to ensure assets are appropriately protected. A vulnerability assessment will determine if the systems are vulnerable to known exploits but will not determine, for example, if personnel records are being stored on a public server.

There is no absolute standard on security – it is a question of managing risk and this varies between organizations.

For example, consider the password requirements such as minimum/maximum password ages and account lockout policies. There may be very good reasons to change passwords frequently or infrequently. There may also be very good reasons to

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

lock an account out if there have been more than five login failures, but if this is a mission critical system, setting something higher might be more prudent or even disabling lockouts altogether.

These configuration settings have much to do with system management and security policy, but not specifically system vulnerabilities or missing patches. Nessus can perform compliance checks for Unix and Windows servers. Policies can be either very simple or very complex depending on the requirements of each individual compliance scan.

Audit vs. Vulnerability Scan

Nessus can perform vulnerability scans of network services as well as log into servers to discover any missing patches. However, a lack of vulnerabilities does not mean the servers are configured correctly or are "compliant" with a particular standard.

The advantage of using Nessus to perform vulnerability scans and compliance audits is that all of this data can be obtained at one time. Knowing how a server is configured, how it is patched and what vulnerabilities are present can help determine measures to mitigate risk.

At a higher level, if this information is aggregated for an entire network or asset class (as with Tenable's SecurityCenter), security and risk can be analyzed globally. This allows auditors and network managers to spot trends in non-compliant systems and adjust controls to fix these on a larger scale.

Example Audit Items

The sections below discuss configuration audits on Windows, Unix, databases, IBM iSeries, and Cisco systems.

The Nessus 5 regex engine is based on a Perl dialect and considered "Extended POSIX", due to its flexibility and speed.

All audit files must be encoded in ANSI format. Unicode, Unicode big endian, and UTF-8 encoded files will not work.

Windows

Nessus can test for any setting that can be configured as a "policy" under the Microsoft Windows framework. There are several hundred registry settings that can be audited and the permissions of files, directories, and objects can also be analyzed. A partial list of example audits includes testing the settings of the following:

- Account lockout duration
- Retain security log
- Allow log on locally
- Enforce Password History

Following is an example "audit" item for Windows servers:

```
<item>
 name: "Minimum password length"
 value: 7
</item>
```

This particular audit looks for the setting "Minimum password length" on a Windows server and generates an alert if the value is less than seven characters.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Nessus can also search Windows computers for sensitive data. Following is an example that searches for Visa credit card numbers in a variety of file formats:

```
<item>
 type: FILE_CONTENT_CHECK
 description: "Determine if a file contains a valid VISA Credit Card Number"
 file_extension: "xls" | "pdf" | "txt"
 regex: "([^0-9-]|^)(4[0-9]{3}( |-|)([0-9]{4})( |-|)([0-9]{4})( |-|)([0-9]{4}))([^0-9-
       ]|$)"
 expect: "VISA" | "credit" | "Visa" | "CCN"
 max_size: "50K"
 only_show: "4"
</item>
```

This check looks at Excel, Adobe, and text files for patterns that indicate one or more valid Visa credit card numbers are present.

Unix

Nessus can broadly be used to test for permissions of files, content of a file, running processes, and user access control for a variety of Unix-based systems. Currently, checks are available to audit Solaris, Red Hat, AIX, HP-UX, SuSE, Gentoo, and FreeBSD derivatives of Unix.

```
<item>
 name: "min_password_length"
 description: "Minimum password length"
 value: "14..MAX"
</item>
```

This audit checks whether the minimum password length on a Unix system is 14 characters.

Cisco

Nessus can test the running configuration for systems running the Cisco IOS operating system and confirm that it is in accordance with security policy standards. Checks can be performed via a non-privileged login or one utilizing the privileged “enable” password.

```
<item>
 type: CONFIG_CHECK
 description: "Require AAA service"
 info: "Verify centralized authentication, authorization and accounting"
 info: "(AAA)service (new-model) is enabled."
 item: "aaa new-model"
</item>
```

Huawei

Nessus can test the running configuration for systems running the Huawei VRP operating system and confirm that it is in accordance with security policy standards. Checks can be performed via a non-privileged login or one utilizing the privileged “enable” password.

```
<custom_item>
```

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

```
 description: "Huawei: Set super password"
 info: "Set super password for managment levels of 3-15."
 solution: "In system view, run the following command to configure super password :\n
       super password level <level> encryption-type cipher <password>"
 reference: "SANS-CSC|10,PCI|2.2.4,COBIT5|BAI10.01,800-53|CM-2"
 expect: "^super password level ([3-9]|1[0-5]) cipher"
</custom_item>
```

Palo Alto Firewall

Nessus utilizes XSL Transforms (XSLT) and a native API to request information from PAN-OS based Palo Alto devices. Requests are made via the HTTP or HTTPS interface of the firewall, and require `Superuser` or `Superuser (readonly)` administrator credentials for PAN-OS >= 4.1.0, and `Superuser` administrator credentials on PAN-OS < 4.1.0. This allows you to perform audits against an `operational config` on the device.

```
<custom_item>
 type: AUDIT_XML
 description: "Palo Alto Security Settings - 'fips-mode = on'"
 info: "Fips-mode should be enabled."
 api_request_type: "op"
 request: "<show><fips-mode></fips-mode></show>"
 xsl_stmt: "<xsl:template match=\"/\">"
 xsl_stmt: "  <xsl:apply-templates select=\"//result\"/>"
 xsl_stmt: "</xsl:template>"
 xsl_stmt: "<xsl:template match=\"//result\">"
 xsl_stmt: "fips-mode: <xsl:value-of select=\"text()\"/>"
 regex: "fips-mode:[\\s\\t]+"
 expect: "fips-mode:[\\s\\t]+on"
</custom_item>
```

IBM iSeries

Using supplied credentials, Nessus can test the configuration for systems running IBM iSeries and confirm that it is in accordance with security policy standards.

```
<custom_item>
 type: AUDIT_SYSTEMVAL
 systemvalue: "QALWUSRDMN"
 description: "Allow User Domain Objects (QALWUSRDMN) - '*all'"
 value_type: POLICY_TEXT
 value_data: "*all"
 info: "\nref :
       http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415302.pdf
       pg. 21"
</custom_item>
```

NetApp Data ONTAP

Using supplied credentials, Nessus can test the configuration for systems running NetApp Data ONTAP systems and confirm that it is in accordance with security policy standards.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

```
<custom_item>
 type: CONFIG_CHECK
 description: "1.2 Secure Storage Design, Enable Kerberos with NFS -
       'nfs.kerberos.enable = on'"
 info: "NetApp recommends the use of security features in IP storage protocols to
       secure client access"
 solution: "Enable Kerberos with NFS"
 reference: "PCI|2.2.3"
 see_also: "http://media.netapp.com/documents/tr-3649.pdf"
 regex: "nfs.kerberos.enable[\\s\\t]+"
 expect: "nfs.kerberos.enable[\\s\\t]+on"
</custom_item>
```

Salesforce

By leveraging the SOAP API, Nessus can test for a variety of issues in a Salesforce database. For example, this query returns information from the PermissionSet assigned to the user, crossing two tables/object types.

```
<custom_item>
 description: "List user names and whether the permission set assigned to them
       prevents password expiration"
 query: "SELECT Name, (SELECT PermissionSet.PermissionsPasswordNeverExpires FROM
       PermissionSetAssignments) FROM User"
</custom_item>
```

Databases

Nessus can be configured to log into the following database types and determine local security policy compliance:

- SQL Server
- Oracle
- MySQL
- PostgreSQL
- DB2
- Informix/DRDA
- MongoDB

In general Tenable recommends running a database compliance scan with a user having SYSDBA privileges for Oracle, "**sa**" or an account with sysadmin server role for MS-SQL, and DB2 instance user account for DB2 to ensure completeness of the report as some system or hidden tables and parameters can only be accessed by an account with such privileges. For MongoDB, a NoSQL database, Tenable recommends running a database compliance scan with the database user for the associated database.Note that for Oracle, in most cases a user assigned the DBA role will perform most of the checks in Tenable audits, but some checks will report errors because of insufficient access privileges. This same argument is applicable to other databases as well; a lesser privilege account could be used for database auditing but the downside is a complete report cannot be ensured.

Database audits are normally comprised of select statements that retrieve security-related details from your database such as the existence or status of insecure stored procedures. Here is an example that determines if the potentially dangerous "**xp_cmdshell**" stored procedure is enabled:

```
<custom_item>
 type: SQL_POLICY
```

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

```
  description: "xp_cmdshell option"
  info: "The xp_cmdshell extended stored procedures allows execution of host
        executables outside the controls of database access permissions and may be
        exploited by malicious users."
  info: "Checking that the xp_cmdshell stored procedure is set to '0'"
  sql_request: "select value_in_use from sys.configurations where name = 'xp_cmdshell'"
  sql_types: POLICY_INTEGER
  sql_expect: "0"
</custom_item>
```

The ability to write audit files for each organization and search for sensitive data is very useful. This document describes how to create custom policies to look for various types of data.

Audit Reports

When an audit is performed, Nessus attempts to determine if the host is compliant, non-compliant or if the results are inconclusive.

Compliance results in Nessus are logged as “Pass”, “Fail”, and “Warning”. The Nessus user interface and Tenable’s SecurityCenter log results as “Info” for passed, “High” for failed, and “Medium” for inconclusive (e.g., a permissions check for a file that is not found on the system).

Unlike a vulnerability check that only reports if the vulnerability is actually present, a compliance check always reports something. This way, the data can be used as the basis of an audit report to show that a host passed or failed a specific test, or if it could not be properly tested.

Credentialed Scanning and Privileged Account Use

Tenable provides authenticated vulnerability and configuration assessments of systems to validate the presence of vulnerabilities, patches and secure configurations. To obtain accurate results when assessing a system, privileged authentication and access levels must be granted for Nessus or SecurityCenter systems to access the end system. Performing a vulnerability scan or audit with an account lacking sufficient privileges may result in incomplete results. For example, files may not be found and commands may return erroneous or incomplete information or lack output altogether. Configuration of administrator or root-equivalent accounts will avoid erroneous or inaccurate system assessments.

While customers may create accounts with customized privileges for use in scanning and assessment, this approach is fragile and not recommended. The methods used by Tenable’s products to assess systems may change to adapt to new technologies or vulnerabilities; therefore, the required granular privileges may also change.

Considerations when reviewing strategies for authenticated assessment of systems in your environment include:

1. Implement compensating controls for privileged accounts to limit risk, such as:
    a. Log monitoring for when the account is in use outside of standard change control hours, with alerts for activities outside of normal windows.
    b. Perform frequent password rotation for privileged accounts more often than the “normal” internal standard.
    c. Enable accounts only when the time window for scans is active; disable accounts at other times.
    d. On non-Windows systems, do not allow remote root logins. Configure your scans to utilize escalation such as su, sudo, pbrun, .k5login, or dzdo.
    e. Use key authentication instead of password authentication.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

2. Use Nessus Agents where available.
3. If an exception is not granted with the use of compensating controls, perform a scan with an account having lower privileges than what Tenable recommends and observe any missing results. Modify the account privileges so that no missing results are observed.
    a. Changes to the audit file or plug-ins may impact results at a later time.

For further information on credentialed checks please see Appendix A in the Nessus User Guide.

Technology Required

Mobile Device Management (MDM) Compliance Nessus Plugin

Tenable has authored a single Nessus plugin (ID 81914) named "MDM Compliance Checks" that implements the APIs used to audit AirWatch and MobileIron systems. The plugin is pre-compiled with the Nessus "`.nbin`" format. The plugin and corresponding audit policies are available to commercial customers and SecurityCenter users.

Rackspace Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 79356) named Rackspace Compliance Checks. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Cloud Services**" and then the "**Rackspace**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Unix and Windows Configuration Compliance Nessus Plugins

Tenable has authored two Nessus plugins (IDs 21156 and 21157) that implement the APIs used to perform audits against Unix and Windows systems. The plugins have been pre-compiled with the Nessus "`.nbin`" format.

These plugins and the corresponding audit policies are available to commercial customers and SecurityCenter users. This paper also discusses two Windows tools to help create custom Windows `.audit` files and one tool for Unix to create Unix `.audit` files.

For Unix compliance audits, only SSH authentication is supported. Legacy protocols such as Telnet are not permitted for security reasons.

Unix and Windows Content Compliance Nessus Plugin

Tenable has authored a pair of Nessus plugins, named "Windows File Contents Check" (ID 24760) and "Unix File Contents Compliance Check" (ID 72095) that audit Windows and Unix systems for non-compliant content such as PII (Personally Identifiable Information) or PHI (Protected Health Information). The plugins are pre-compiled with the Nessus "`.nbin`" format. The plugins and corresponding audit policies are available to commercial customers and SecurityCenter users.

Unix content checks are supported on Red Hat, SunOS/Solaris, AIX, HP-UX, Mac OS X, FreeBSD, NetBSD, and OpenBSD.

Credit cards numbers not verified by a Luhn algorithm are in most cases false positives. Nessus uses the Luhn algorithm to validate credit card numbers.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Database Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 33814) named "Database Compliance Checks" that implements the APIs used to audit various database systems. The plugin is pre-compiled with the Nessus "`.nbin`" format. The plugin and corresponding audit policies are available to commercial customers and SecurityCenter users.

Database compliance checks are not available for use with Security Center version 3.4.3 and earlier.

IBM iSeries Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 57860) named "IBM iSeries Compliance Checks" that implements the APIs used to audit systems running IBM iSeries. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Miscellaneous**" and then the "**IBM iSeries**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

To perform a successful compliance scan against an iSeries system, authenticated users must have privileges as defined below:

1. A user with (*ALLOBJ) or audit (*AUDIT) authority can audit all system values. Such a user typically belongs to class (*SECOFR).
2. Users of class (*USER) or (*SYSOPR) can audit most values, except QAUDCTL, QAUDENDACN, QAUDFRCLVL, QAUDLVL, QAUDLVL2, and QCRTOBJAUD.

If a user does not have privileges to access a value, then the value returned will be *NOTAVL.

Cisco Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 46689) named "Cisco IOS Compliance Checks" that implements the APIs used to audit systems running the CISCO IOS operating system. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers. This compliance check can be run against a Saved, Running or Startup configuration.

Juniper Junos Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 62680) named "Juniper Junos Compliance Checks" that implements the APIs used to audit systems running the Junos operating system. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers. This compliance check can be run against a running or saved configuration.

Huawei Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 73157) named "Huawei VRP Compliance Checks" that implements the APIs used to audit systems running the Huawei VRP operating system. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

plugin and corresponding audit policies are available to commercial customers. This compliance check can be run against a saved or running configuration.

Palo Alto Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 64095) named "Palo Alto Networks PAN-OS Compliance Checks" that implements the APIs used to audit systems running Palo Alto devices. In addition, a Nessus plugin (ID 64286) named "Palo Alto Networks Settings" is used to configure authentication information required to perform the audit. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Miscellaneous**" and then the "**Palo Alto Networks PAN-OS**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

VMware Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 64455) named "VMware vCenter/vSphere Compliance Checks" that implement the VMware SOAP API to audit ESX, ESXi, and vCenter software. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Miscallaneous**" and then the "**VMware ESX SOAP API**" or "**VMware cVenter SOAP API**" sub-tabs. The plugin and corresponding audit policies are available to commercial customers. For more information on conducting an audit against VMware, consult the associated blog post.

Citrix XenServer Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 69512) named "Citrix XenServer Compliance Checks" that implements the APIs used to audit systems running Citrix XenServer, as well as vendors creating their own versions of XenServer based on open sourced code. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers. For more information on conducting an audit against XenServer, consult the associated blog post.

HP ProCurve Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 70271) named "HP ProCurve Compliance Checks" that implements the APIs used to audit systems running HP's ProCurve. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

FireEye Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 70469) named "FireEye Compliance Checks" that implements the APIs used to audit systems running FireEye systems. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Fortigate FortiOS Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 70272) named "Fortigate FortiOS Compliance Checks" that implements the APIs used to audit systems running FortiOS systems. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Amazon AWS Compliance Capability

Tenable has authored a Nessus plugin (ID 72426) named "Amazon AWS Compliance Checks" that implements the Amazon AWS API used to audit systems running AWS instances. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab.

The AWS Access Key ID, AWS Secret Access Key, and AWS region can be added to the "**Credentials**" tab of a policy under "**Cloud Services**" and then the "**Amazon AWS**" sub-tab. The plugin and corresponding audit policies are available to commercial customers. Nessus only needs `ReadOnly` Access to the account. For this plugin, Tenable recommends creating a new user group with `ReadOnly` Access, and then assigning a new user to that group. When you generate a new user, generate an Access Key ID and Secret Access Key. Those keys are used for setting up the AWS Audit Scan. Running Amazon AWS compliance checks do not require specific permission from AWS to run, as outlined by Amazon.

Dell Force10 Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 72461) named "Dell Force10 FTOS Compliance Checks" that implements the APIs used to audit systems running the Dell Force10 FTOS system. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Adtran AOS Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 71991) named "Adtran AOS Compliance Checks" that implements the APIs used to audit systems running the Adtran operating system (AOS). This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

SonicWALL SonicOS Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 71955) named "SonicWALL SonicOS Compliance Checks" that implements the APIs used to audit systems running the SonicWALL SonicOS. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Extreme ExtremeXOS Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 73156) named "Extreme ExtremeXOS Compliance Checks" that implements the APIs used to audit systems running the Extreme ExtremeXOS. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Check Point GAiA Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 62679) named "Check Point GAiA Compliance Checks" that implements the APIs used to audit systems running the Check Point GAiA OS. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Brocade FabricOS Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 71842) named "Brocade FabricOS Compliance Checks" that implements the APIs used to audit systems running the Brocade Fabric OS (FOS). This plugin is pre-compiled with the Nessus "**`.nbin`**" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

NetApp Data ONTAP Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 66934) named "NetApp Data ONTAP Compliance Checks" that implements the APIs used to audit systems running the NetApp Data ONTAP filer. This plugin is pre-compiled with the Nessus "**`.nbin`**" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Host**" and then the "**SSH**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

SCAP Linux and Windows Compliance Checks

Tenable has authored two Nessus plugins (ID 66756 and ID 66757) named "SCAP Windows Compliance Checks" and "SCAP Linux Compliance Checks", respectively, that implements the APIs used to audit systems against the policy specified by Security Content Automation Protocol (SCAP) content. For more information, see the Nessus v6 SCAP Assessments document.

MongoDB Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 76513) named "MongoDB Compliance Checks" that that implements the MongoDB driver used to audit systems running the MongoDB NoSQL database. This plugin is pre-compiled with the Nessus "**`.nbin`**" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Database**" and then the "**MongoDB**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

MongoDB compliance checks are not available for use with Nessus versions earlier than 5.2.

Salesforce Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 76711) named "Salesforce.com Compliance Checks" that implements the SOAP APIs used to audit databases on the Salesforce network. This plugin is pre-compiled with the Nessus "**`.nbin`**" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Cloud Services**" and then the "**Salesforce.com**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

BlueCoat ProxySG Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 70470) named "BlueCoat ProxySG Compliance Checks" that implements the SOAP APIs used to audit systems on a BlueCoat ProxySG appliance. This plugin is pre-compiled with the Nessus "**`.nbin`**" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**????**" and then the "**????**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Red Hat Enterprise Virtualization (RHEV) Compliance Nessus Plugin

Tenable has authored a Nessus plugin (ID 77090) named "RHEV Compliance Checks" that implements the APIs used to audit systems running Red Hat Enterprise Virtualization. This plugin is pre-compiled with the Nessus "`.nbin`" format and a Tenable-provided "best practices" audit is available in the plugin feed, or you can upload your own via the "**Compliance**" tab. Credential information can be added to the "**Credentials**" tab of a policy under "**Miscellaneous**" and then the "**RHEV**" sub-tab. The plugin and corresponding audit policies are available to commercial customers.

Audit Policies

Tenable has developed a number of different audit policies for Unix, Windows, Palo Alto, IBM iSeries, VMware, and Cisco platforms. These are available as `.audit` text files to commercial subscribers and can be downloaded from the Tenable Support Portal located at https://support.tenable.com/. For the latest news regarding Tenable's auditing functionality and all of the latest `.audit` file releases, please see the Discussion Forums: https://discussions.nessus.org/.

Many aspects of common compliance audits such as the requirements of SOX, FISMA, and PCI DSS have been considered while writing these audit policies, though they are not represented as official audit files for these criteria. Users are encouraged to review these `.audit` policies and customize these checks for their local environment. Users may rename the `.audit` files to suit local descriptions. Other `.audit` policies come directly from recommended configuration settings by CERT, CIS, NSA, and NIST.

Tenable expects to author several different types of `.audit` files based on customer feedback and evolving "best practices". Several consulting organizations and Tenable customers have also begun to implement their own `.audit` policies and have expressed interest to share these with other Nessus commercial users. An easy way to share `.audit` policies or just interact with the Nessus community is through the Tenable Network Security Discussion Forums at https://discussions.nessus.org/.

Helpful Utilities

Tenable has developed a tool to convert `.inf` files to Nessus `.audit` files to perform Windows audits. This tool is named `i2a` and is also discussed later in this document.

There are two Unix tools that can be used to create Unix `.audit` files. The first tool, named `c2a` (for "configuration to audit"), can be used to create Unix `.audit` files directly from existing configuration files. For example, if your Sendmail configuration file is configured correctly according to your site policy, the `c2a` tool can create an audit policy based on the MD5 checksum of the file or based on specific value and argument pairs in the `sendmail.cf` file. The second tool, named `p2a` (for "package to audit"), can be used to create Unix `.audit` files from either the base package set on a Unix (RPM-based Linux or Solaris 10) system or from a flat text file with a list of package names.

Unix or Windows Nessus Scanners

A variety of platforms can be used to run compliance checks and generally, the underlying operating system that Nessus resides on does not matter. You can perform compliance audits of a Windows 2003 server from an OS X laptop and you can also audit a Solaris server from a Windows laptop.

Credentials for Devices to be Audited

In all cases, Unix SSH, Windows Domain, IBM iSeries, Cisco IOS, or database credentials are required for Nessus to log into the target servers. In most cases, this user must be a "Super user" or be a regular user with privilege escalation ability (e.g., `sudo`, `su` or `su+sudo`). If the user performing the audit does not have "Super user" privileges, many of the remote system commands will not be able to be run or will return incorrect results.

The Windows account used for sign-on credentials must have permission to read the local machine policy. If a target host does not participate in a Windows domain then the account must be a member of the host's administrators group. If the host participates in a domain, then the domain's administrator group will be a member of the host's administrators group and the account will have access to the local machine policy if it is a member of the domain's administrator group.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

To perform Windows content compliance checks, in addition to logging in to the system with domain privileges, access to the Windows Management Instrumentation (WMI) must also be allowed. If this access is not available, Nessus will state that WMI access was not available for the scan.

Database compliance checks require only the database credentials to perform a full database compliance audit. This is because the database, not the host operating system, is being scanned for compliance.

Cisco IOS compliance checks typically require the "enable" password to perform a full compliance audit of the system configuration. This is because Nessus is auditing the output of the "**`show config`**" command, available only to a privileged user. If the Nessus user being used for the audit already has "enable" privileges, the "enable" password is not required.

For more information on configuring Nessus or SecurityCenter to perform local credentialed vulnerability checks, please refer to the "Nessus Credentials Checks for Unix and Windows" paper available at http://www.tenable.com/products/nessus/documentation.

Using "su", "sudo", and "su+sudo" for Audits

Use "**`su+sudo`**" in cases where company policy prohibits Nessus from logging into a remote host with the root user or a user with "**`sudo`**" privileges. On remote login, the non-privileged Nessus user can "**`su`**" (switch user) to one with **`sudo`** privileges.

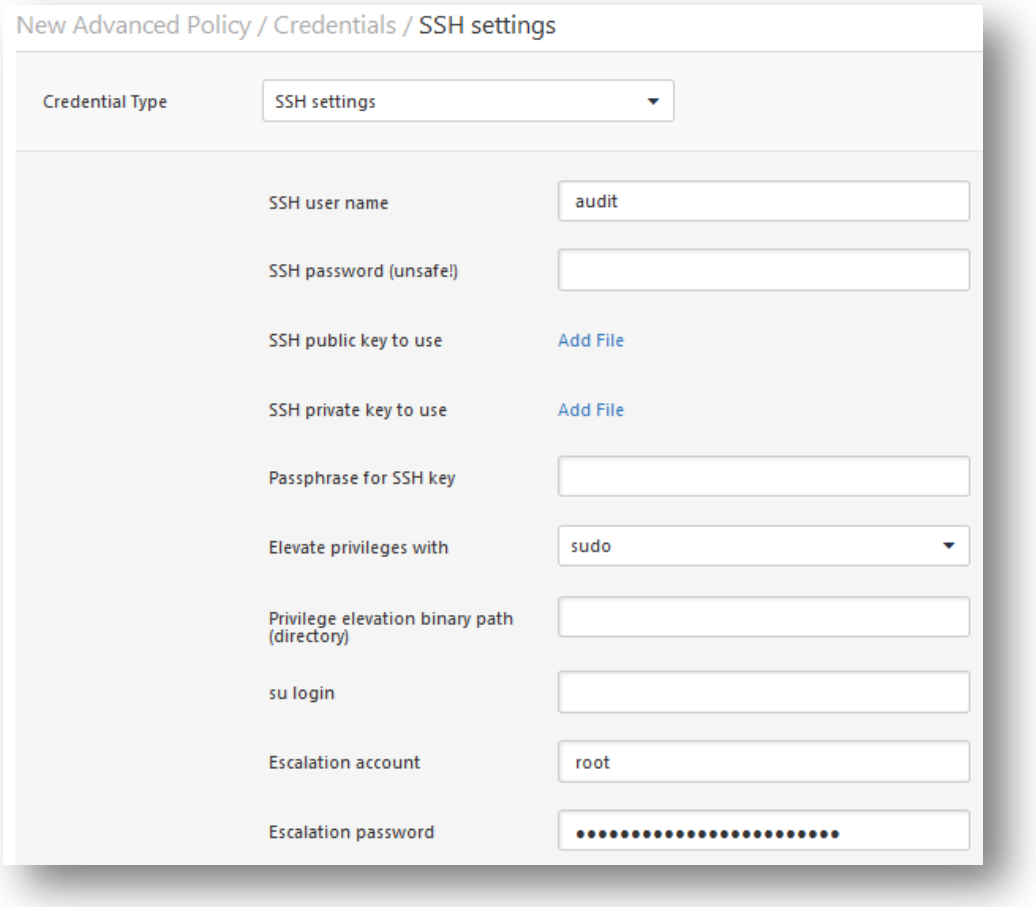
The most effective Unix credentialed scans are those when the supplied credentials have "root" privileges. Since many sites do not permit a remote login as root, Nessus users can now invoke "**`su`**", "**`sudo`**", or "**`su+sudo`**" with a separate password for an account that has been set up to have the appropriate privileges.

In addition, if an SSH **`known_hosts`** file is available and provided as part of the scan policy, Nessus will only attempt to log into hosts in this file. This ensures that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

sudo Example

An example screen capture of using "**sudo**" in conjunction with SSH keys follows. For this example, the user account is "audit", which has been added to the **/etc/sudoers** file on the system to be scanned. The password provided is the password for the "audit" account, not the root password. The SSH keys correspond with keys generated for the "audit" account:



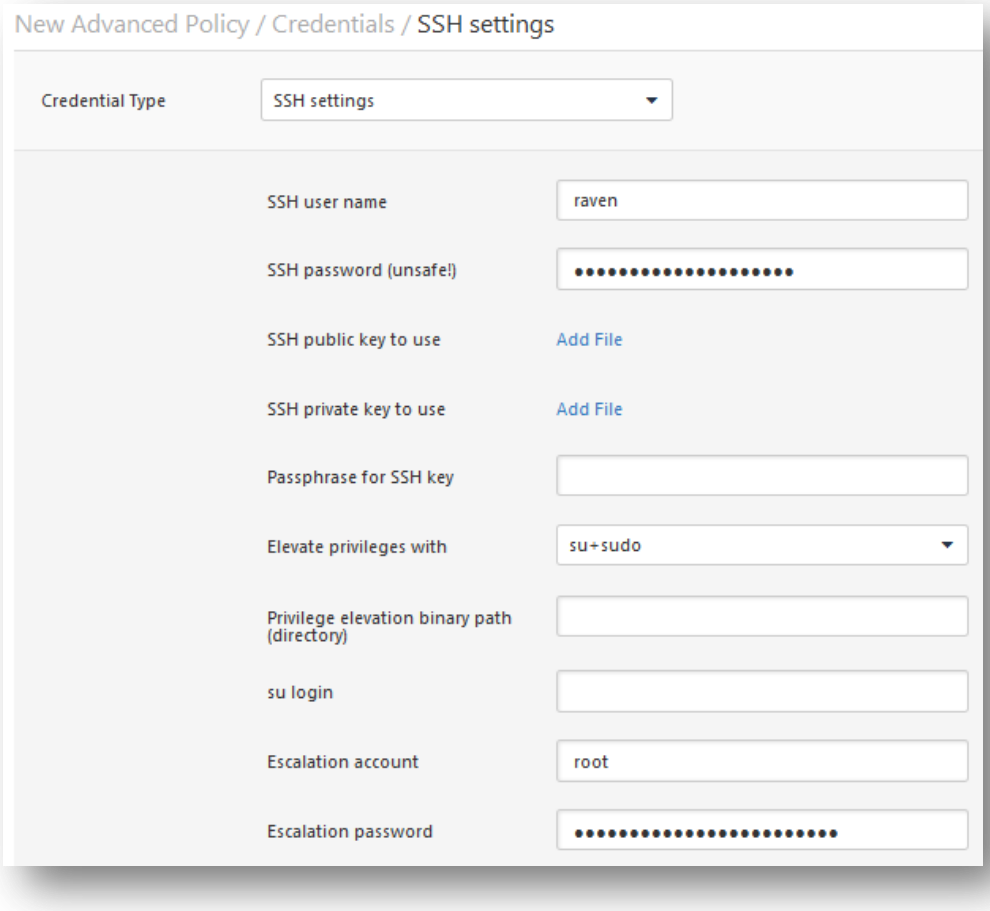
su+sudo Example

With the release of Nessus 4.2.2, a new method of credential elevation has been included for Unix-based hosts that have **sudo** installed: "**su+sudo**". This method allows you to provide credentials for an account that does not have **sudo** permissions, **su** to a user account that does and then issue the **sudo** command.

This configuration provides greater security for your credentials during scanning, and satisfies compliance requirements for many organizations.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

To enable this feature, simply select "su+sudo" in the "Elevate privileges with" section under the credentials/SSH settings as shown in the following screen capture:



In the "SSH user name" and "SSH password" fields, enter the credentials that do not have **sudo** privileges. In the example above, the user account is "raven." From the "Elevate privileges with" pull-down menu, select "su+sudo". In the "su login" and "Escalation password" fields enter the user name and password that *do* have privileged credentials, in this example "sumi". No other scan policy changes are required.

Important Note Regarding sudo

When auditing Unix systems via **su**, **sudo**, or **su+sudo**, please keep the following items in mind:

- If your Unix system has been hardened to limit which commands can be executed via **sudo** or files accessed by remote users, this may affect your audit. Compare non-root audits with a root audit if you suspect the audit is being limited by security measures.
- The **sudo** command is not native to Solaris and needs to be downloaded and installed if your target system is running Solaris. Make sure the **sudo** binary is accessible as "**/usr/bin/sudo**".
- When scanning with **known_hosts**, the Nessus scan still needs to specify a host to be scanned as well. For example, if you scanned a class C but uploaded a **known_hosts** file that only contained 20 individual hosts within that class C, Nessus would just scan those hosts in the file.
- Some Unix-based configurations have a requirement that sudo-initiated commands be performed from **tty** sessions. Nessus vulnerability scans performed with the "**su+sudo**" option do not match that requirement. If you are

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

using the "**su+sudo**" option you will need to create an exception on the target system. To determine if this is the case for your Unix distribution, enter the following command as root on the system you will be scanning:

```
# grep requiretty `locate sudoers` | grep -v "#" | grep /etc
```

If the "**requiretty**" line is in the **sudoers** configuration file, an exception to this rule will need to be made to the **/etc/sudoers** file as follows:

```
Defaults    requiretty
Defaults:{userid} !requiretty
```

Note that {userid} is the username that will be used to execute the "**sudo**" command (the "su login" page in the credentials/SSH section of your policy). Also make sure you have the following line in your **sudoers** file:

```
{userid}     ALL=(ALL)       ALL
```

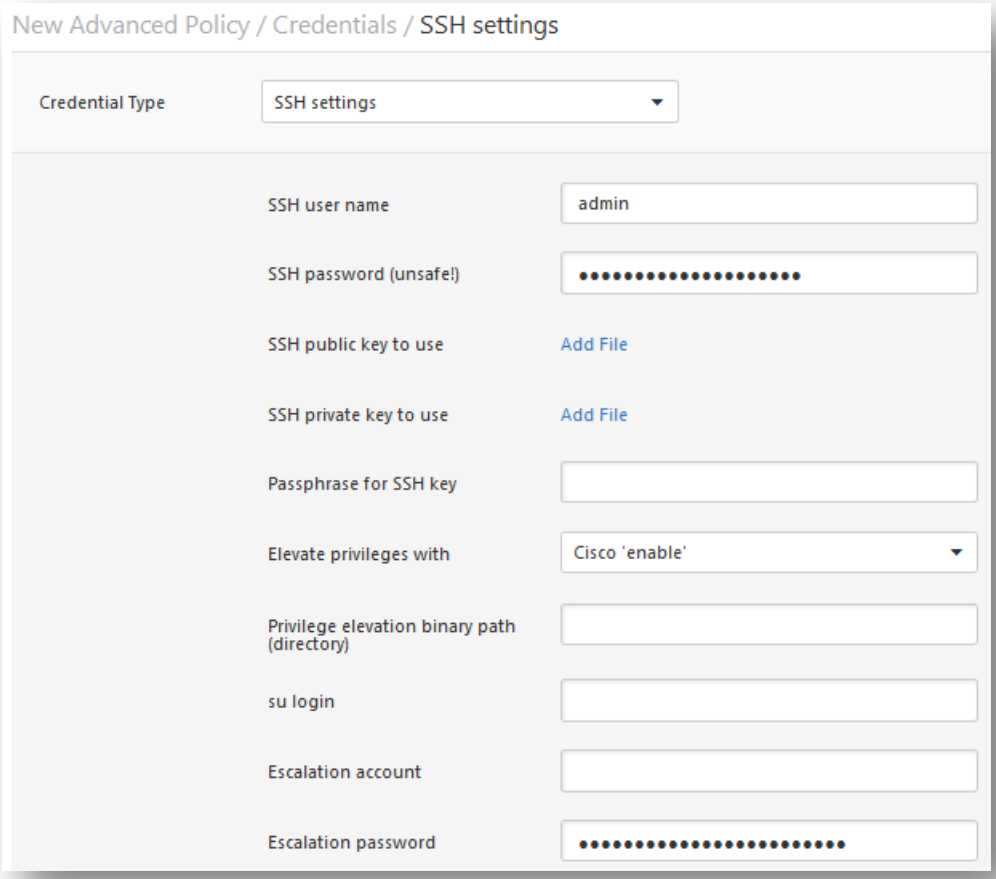
Again, {userid} is the username that will be used to execute the "**sudo**" command (the "su login" in the credentials/SSH section of your policy).

Cisco IOS Example:

Only SSH authentication is supported. Legacy IOS devices requiring Telnet for authentication cannot be scanned with Nessus Cisco compliance checks.

The Cisco IOS credentials are configured via the "**SSH settings**" credential screen in the Nessus user interface. Enter the SSH username and password required to log into the Cisco router. To specify that privileges must be elevated with "Enable", choose "**Cisco 'enable'**" next to the "**Elevate privileges with**" setting and enter the enable password next to "**Escalation password**".

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.



Converting Windows .inf Files to .audit Files with i2a

If you or your IT organization has possession of Windows policy files (commonly found with the "`.inf`" extension) these can be converted into `.audit` files for use in Nessus audits of Windows servers.

Obtaining and Installing the Tool

The `i2a` tool is available as a zip file and can be obtained from the Tenable Support Portal located at https://support.tenable.com/. This tool does not use a GUI and is run from the command line.

Extract the contents of the file into a directory of your choosing and then move your Windows `.inf` files into the same directory.

Converting the .inf to .audit

Run the conversion tool from the command prompt by simply typing:

```
# i2a-x.x.x.exe yourfile.inf file.audit
```

In this example `yourfile.inf` is the source `.inf` file and `file.audit` is the target `.audit` file.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Analyzing the Conversion

Tenable has attempted to achieve as close to 100% of a conversion between what can be described in an **.inf** file and what can be audited for in an **.audit** file. However, there are a few policy items that cannot be tested for with the current Nessus 5 technology.

A log of the conversion process is created for each run of the **i2a** tool. It contains a line by line audit of the entire conversion process. If a line in the **.inf** cannot be converted, it will be contained in this log file.

Correct .inf Setting Format

For the checks shown in the log file that could not be processed, please make sure they conform to the acceptable formats listed below.

System Access, **System Log**, **Security Log**, **Application Log**, and **Event Audit** settings share the same format. Each entry is described by the "**Key**" followed by a "**value**".

Syntax:

```
Key = value
```

In the above case, **Key** is the item to be audited and **value** is the expected value for that key on the remote system.

Example:

```
MinimumPasswordLength = 8
```

The format for **Privilege Rights** settings is similar to the one mentioned above, however in this setting the value can be empty.

Syntax:

```
PriviledgeRight = User1,User2…UserN
```

Example:

```
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-544
```

Or:

```
SeTcbPrivilege =
```

A **Registry Key** setting consists of the following four parts:

- Registry Key – The Registry key that needs to be audited.
- Inheritance Value – Identifies whether the permissions for this registry key are inherited or not inherited. The value can be [0-4].

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

- DACL – DACL is an ACL that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.
- SACL – SACL is an ACL that controls the generation of audit messages for attempts to access a securable object.

Syntax:

```
"Registry Key",Inheritance value,
"D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)... (string_acen)"
```

DACL and SACL fields may be empty, in which case the check will be ignored.

Example:

```
"MACHINE\SYSTEM\CurrentControlSet\Control\Class",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)
      S:PAR(AU;OICIFA;CC;;;WD)"
```

The format for **File Security** setting is similar to the Registry Key format described above.

Syntax:

```
"File Object",Inheritance value,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...
      (string_acen)"
```

Example:

```
"%SystemRoot%\system32\ciadv.msc",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICI
      FA;CC;;;WD)"
```

The **Service General** setting consists of the following four parts:

- Service Name – The service that needs to be audited.
- Service start type – Manual, Automatic, or Disabled. The value can be [2-4].
- DACL – DACL is an ACL that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.
- SACL – SACL is an ACL that controls the generation of audit messages for attempts to access a securable object.

Syntax:

```
Service Name,Start type,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...(string_a
      cen)"
```

Example:

```
kdc,3,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLO
      CRRC;;;SY)"
```

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

If the permissions for a service setting are not required to be checked and only the startup type needs to be audited, it can be done as follows.

Syntax:

```
Service Name,Start type
```

Example:

```
kdc,3,""
```

The **Registry Value** setting consists of the following three parts:

- RegistryKey – The Registry key that needs to be audited.
- RegistryType – The registry type: REG_DWORD, REG_SZ, etc.
- RegistryValue – Value for the registry key.

RegistryValue may be defined in double, single, or without quotes.

Syntax:

```
RegistryKey,RegistryType,RegistryValue
```

Example:

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
```

If it is desired to comment a particular line within the **.inf** file, please append a semicolon ";" in front of the line and the script will ignore that line.

Converting Unix Configuration Files to .audit Files with c2a

The **c2a.pl** tool is designed to assist auditors in creating **.audit** files to audit application configurations on a given network. For example, if it is desired that all the web servers on a given network must be configured exactly as the master host X, then in that case one would run this tool on host X, create the **.audit** file for **httpd** on that system and then input this file to the Nessus daemon and run the scan against all the other web servers to check for compliance.

Optionally, this tool can also be used to create MD5 audit files for an entire host. It expects a list of files/directories that need to be audited in an input file, which it then processes recursively in the case of directories to create an **.audit** file for the system. This file can then be used at a later date to scan for changes to core files and directories.

Obtaining and Installing the Tool

The **c2a** tool is a compressed **tar** archive and can be obtained from the Tenable Support Portal located at https://support.tenable.com/.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Extract the contents of **c2a-x.x.x.tar.gz** on your local machine with the following command:

```
# tar xzf c2a-x.x.x.tar.gz
```

This will create a "**c2a**" directory under the current directory and extract the files into it. If you would like to extract the contents to a directory of your choice, use the following command:

```
# tar xzf c2a.x.x.x.tar.gz -C /path/to/directory
```

After uncompressing the archive you should see the following files under the **~/c2a** directory:

- **c2a.pl**
- **c2a.map**
- **c2a_regex.map**
- **cmv.pl**
- **ReadMe.txt**

Create a MD5 Audit File

Run the conversion tool with the "**-md5**" option by typing:

```
# ./c2a.pl -md5 -f /path/to/inputfile.txt -o outputfile.audit
```

The tool expects an input file with a list of files and directories that need to be audited for MD5 values as well as an output filename for the audit file.

When adding files to your input file please remember to use this format:

`/path/to/file`

Use this format when adding directories:

`/path/to/file/`

If this format is used and the file is an actual file and not a directory, the `c2a` tool will complain about this file not existing. The leading slash "/" is completely fine for adding directories.

If the entry in the input file is a normal MD5 file, only that file will be computed and written to the **.audit** format. In the case of a directory, the script will delve recursively into each and every file of that directory. If an output file is not specified, the result will be written to **~/c2a/op.audit**.

When processing the list of files specified by the "inputfile", any symbolic links encountered will be ignored. A warning message will appear stating either the file does not exist or it is a symbolic link. As of this version, **c2a** does not support symbolic links.

Create Audit File Based on One or More Configuration Files

The **c2a** tool is ideal for processing configuration files that have unique line-by-line content. If your configuration file has multi-line functionality, such as an XML configuration file, **c2a** is not ideal.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Run the conversion tool with the "**-audit**" option by typing:

```
# ./c2a.pl -audit -f /path/to/input.txt -o outputfile.audit
```

The tool expects an input file (**input.txt**) that contains a list of configuration files that need to be audited, as well as an output filename for the audit file.

The **c2a.pl** Perl script relies on two key files: **c2a.map** and **c2a_regex.map**. It scans each line of a configuration file that is being audited and checks if the first word on that line matches for the "type" in the **c2a.map** file (e.g., HTTP, SENDMAIL, etc.), and the value that is associated with it. For example, if it is auditing HTTP settings, it checks if the word matches any of the HTTP keywords in the **c2a.map** file. If it does, it applies the regex expression from **c2a_regex.map** for HTTP to that line and extracts the setting and the value. Only those settings for which an entry exists in **c2a.map** will be audited.

Configuration files that are not desired to be audited can be commented using the "#" character.

If it is desired to convert settings that have been commented out in the configuration file into **.audit** format, please edit the **c2a.pl** and set "`$ENFORCE_COMMENT = 1;`".

As in the earlier case, if the output file is not specified, the result will be written to **~/c2a/op.audit**.

Currently, Tenable provides MAP settings for HTTP, SENDMAIL, SYSCTL, and NESSUS. Additional applications settings can be easily added by making use of a **cmv.pl** Perl script. Please refer to the next section for more information.

Creating a MAP File

Creating a MAP file for an application is simple. Just run the **cmv.pl** script as follows:

```
# ./cmv.pl -r 'regex' -r tag -f config_file
```

Where:

- "**regex**" is the regex to extract the configuration setting and value pair. Typically this is of the form "<name> = <value>". But in some cases it might be slightly different, where "=" might be replaced by a space, tab, etc.
- "**tag**" is essentially the keyword that you wish to tag the application being audited. The **tag** keyword links the **config_file** with the keywords in **c2a.map** and regex in **c2a_regex.map** hence it is important that the tag in each of these files is the same.
- "**config_file**" is the file for which a MAP file is being created.

For example, if you want to audit configuration settings for VSFTPD, perform the following steps:

1. First, use **cmv.pl** as follows:

   ```
   # ./cmv.pl -r '([A-Za-z0-9_]+)=([A-Za-z0-9]+)' -t VSFTPD -f /root/vsftpd-0.9.2/vsftpd.conf
   ```

   This will create the **tag.map** file (e.g., **VSFTPD.map**). By default, all lines that have been commented out will be ignored. If you wish to consider all variables, change the **$ENFORCE_COMMENT** value from "0" to "1" and then re-run the script.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

2. Inspect and append the MAP file to **c2a.map**.

   Check the **VSFTPD.map** file for any undesired values that might have inadvertently matched your regex expression. After you have examined all the keywords to be correct, append them to **c2a.map**.

3. Update **c2a_regex.map** with the same expression used by **cmv.pl** as follows:

   ```
   VSFTPD=([A-Za-z0-9_]+)=([A-Za-z0-9]+)
   ```

   Note: it is the same regex expression as used by the **cmv.pl** Perl script.

4. Update **input.txt** with the location of the VSFTPD configuration file:

   ```
   VSFTPD=/root/vsftpd-0.9.2/vsftpd.conf
   ```

5. Run the **c2a.pl** script:

   ```
   # ./c2a.pl -audit -f input.txt
   ```

6. Finally, check the output file:

   ```
   # vi op.audit
   ```

Other Uses for the c2a Tool

Tenable has included several entries in the **c2a.map** and **c2a_regex.map** files to enable auditing of Sendmail, the Very Secure FTP Daemon (VSFTPD), Apache, the Red Hat **/etc/sysctl.conf** file and Nessus. More software may be added in the near future. If you would like to submit new mappings to Tenable to share with other Nessus users, please send them to nessus-support@tenable.com.

With that in mind, the **c2a.pl** script can be used to help create Nessus **.audit** files for several live Unix applications. Consider the following ideas:

- If your organization has many Unix-based firewalls, an **.audit** file can be generated to audit the common and required settings that each firewall is supposed to have. For example, if all firewalls are supposed to have filtering of RFC 1918 addresses, the actual firewall rules can be tested for.
- If many different custom applications are being run out of CRON, the various CRONTABs can be audited to make sure that the right applications are being run at the correct time.
- For centralized logging, remote Unix systems can have their SYSLOG, SYSLOG-NG, and LOGROTATE configurations checked.

Manual Tweaking of the .audit Files

Finally, the output of the **c2a.pl** script can also be manually edited. For example, consider combining the MD5 checksum rules with the FILE_CONTENT_CHECK rules into one rule. The output generated by the **c2a.pl** script also assumes that a configuration file is always in one place. Consider modifying the "**file**" keyword to specify other locations where a configuration file may be located.

If you have content that you do not want in your remote file configurations, consider manually adding in checks for that with the FILE_CONTENT_CHECK_NOT keyword. This can help you perform audits for settings that should be present and should also not be present.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Converting Unix Package Lists to .audit Files with p2a

The **p2a.pl** tool is designed to assist auditors with creating **.audit** files for install package configurations on RPM-based Linux and Solaris 10 systems. For example, if it is desired that all Linux web servers on a given network have the same RPM base as the master host X, then one would run this tool on host X that would create an **.audit** file containing all RPM packages on that system. One would then use this **.audit** file with Nessus to run a scan against other web servers to check for compliance.

Optionally, this tool can be used to create an audit file from a text listing of RPM or Solaris 10 packages. It expects a list of packages, one per line, in an input file and then properly formats an **.audit** file for the target system. The generated **.audit** file can then be used at a later date to scan for changes to core install packages.

Obtaining and Installing the Tool

The **p2a** tool is a compressed **tar** archive comprised of a single Perl script and a **ReadMe.txt** help file. It can be obtained from the Tenable Support Portal located at https://support.tenable.com/.

Extract the contents of **p2a-x.x.x.tar.gz** on your local machine with the following command:

```
# tar xzf p2a-x.x.x.tar.gz
```

This will create a "**p2a**" directory under the current directory and extract the files into it.

If you would like to extract the contents to a directory of your choice, use the following command:

```
# tar xzf p2a.x.x.x.tar.gz -C /path/to/directory
```

After uncompressing the archive you should see the following files under the **~/p2a** directory:

- p2a.pl
- ReadMe.txt

Make the script executable by running:

```
# chmod 750 p2a.pl
```

Usage

Run the Perl script as follows:

```
# ./p2a.pl [-h] -i inputfile.txt -o outputfile.audit
```

The standalone argument "**-h**" is optional and displays the help tool.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Create Output File Based on all Installed Packages

If the script is run solely with "**-o**" option, it runs a system command to extract all locally installed system package names and the resulting **.audit** file will be written to **/path/to/outputfile.audit**.

```
# ./p2a.pl -o /path/to/outputfile.audit
```

Output files must include the **.audit** extension for the script to run. An error indicating improper file extension will be generated otherwise.

Create Output File Based on Package List and Send to the Screen

Run **p2a** to send all resulting output to the terminal window with the following syntax:

```
# ./p2a.pl -i /path/to/inputfile.txt
```

This option requires an input file and will generate output to the terminal window (**stdout**) that can be copied and pasted into your **.audit** file. The input file must be formatted with one package per line and no added delimiters.

Example:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

Because many Unix-based systems can have greater than a thousand installed packages, the amount of output may exceed your scroll buffer and make viewing all output difficult.

Create Audit File Based on a Specified Input File

Running **p2a** with both input and output arguments takes your formatted package listing and generates an **.audit** file in the specified location.

```
# ./p2a.pl -i /path/to/input_file.txt -o /path/to/outputfile.audit
```

Input files must be formatted with one package per line and no added delimiters.

Example:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Output files must include the `.audit` extension for the script to run. An error indicating improper file extension will be generated otherwise.

Example Nessus User Interface Usage

Obtaining the Compliance Checks

Commercial customers will already have the compliance checks for their Nessus scanner and several `.audit` files are available from the Tenable Support Portal located at https://support.tenable.com/. To confirm this, run the Nessus user interface, authenticate, and manage or edit an existing policy. Under the "Plugins" tab look for the family "Policy Compliance", click on the plugin family name and confirm that the following plugins are displayed:

- Cisco IOS Compliance Checks
- Huawei VRP Compliance Checks
- Database Compliance Checks
- IBM iSeries Compliance Checks
- PCI DSS Compliance
- PCI DSS Compliance: Database Reachable from the Internet
- PCI DSS Compliance: Handling False Positives
- PCI DSS Compliance: Insecure Communication Has Been Detected
- PCI DSS Compliance: Remote Access Software Has Been Detected
- PCI DSS Compliance: Passed
- PCI DSS Compliance: Tests Requirements
- Unix Compliance Checks
- Windows Compliance Checks
- Windows File Contents Compliance Checks

Configuring a Scanning Policy

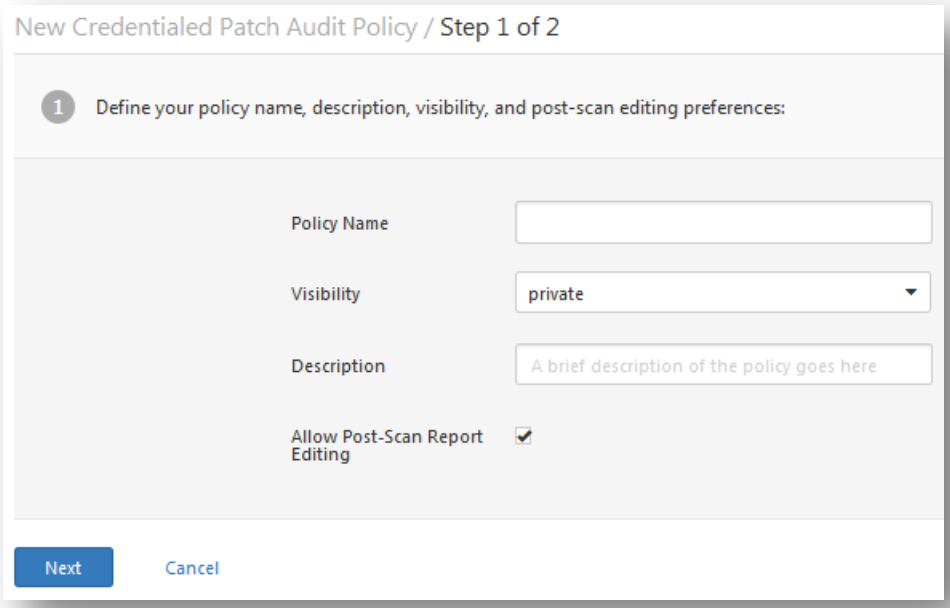
To enable the compliance checks in Nessus, a scanning policy must be created with the following attributes:

- Enable the compliance check plugins that are in the plugin family "Policy Compliance"
- Specify one or more `.audit` compliance policies as a preference
- Specify the credentials to access the target server including database credentials under the "Preferences" tab if applicable
- Enable plugin dependencies

This can be done via the Policy template and selecting the "**Credentialed Patch Audit**" template, or manually via the "**Advanced Policy**".

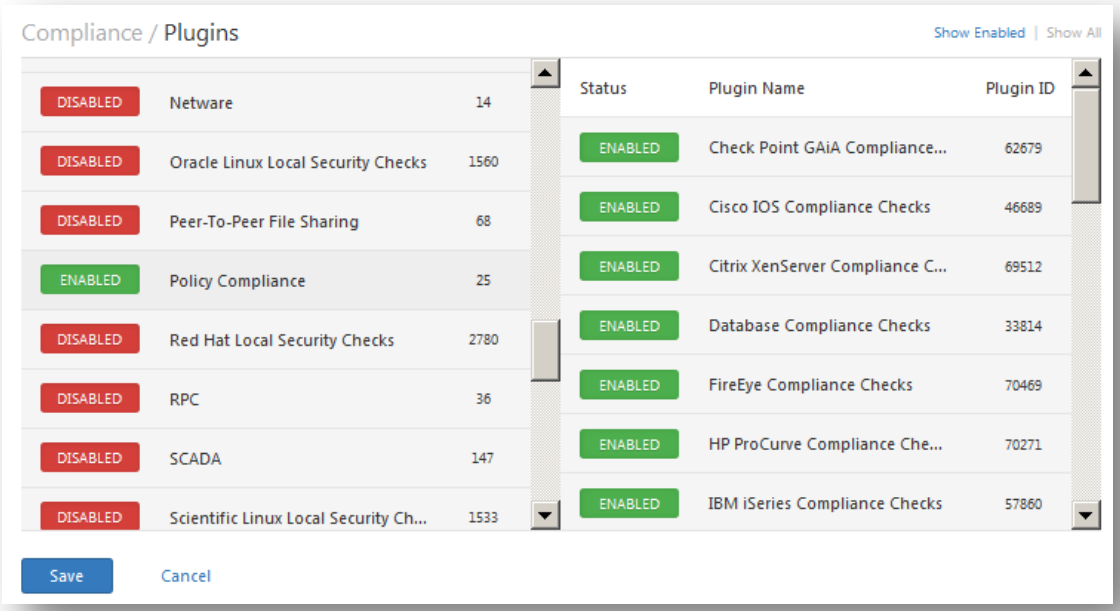
It is important to understand the checks in the `.audit` files you select, especially when custom files have been created. When using two `.audit` files on the same scan, both files are combined to produce the results of each file in one scan. If there are conflicting results between the files, you could receive one passing and one failed result each. Always be sure to verify the findings in your reports.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.



To create a scan policy, access the Nessus user interface, authenticate, and select "Policies". Edit an existing policy or create a new one. You can specify the credentials to access the target server under the "**Credentials**" tab on the left.

Under the "**Plugins**" tab, enable the plugin family "Policy Compliance" and make sure "`auto_enable_dependencies`" is set to "**yes**" in the Advanced Settings (this is the default setting):

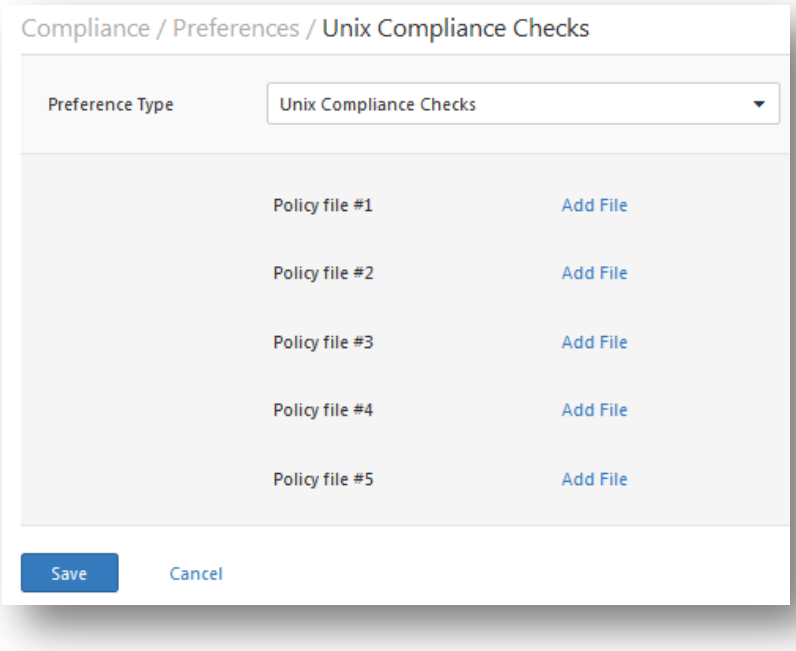

Compliance / Plugins
Show Enabled | Show All
DISABLED Netware 14
DISABLED Oracle Linux Local Security Checks 1560
DISABLED Peer-To-Peer File Sharing 68
ENABLED Policy Compliance 25
DISABLED Red Hat Local Security Checks 2780
DISABLED RPC 36
DISABLED SCADA 147
DISABLED Scientific Linux Local Security Ch... 1533
Status Plugin Name Plugin ID
ENABLED Check Point GAiA Compliance... 62679
ENABLED Cisco IOS Compliance Checks 46689
ENABLED Citrix XenServer Compliance C... 69512
ENABLED Database Compliance Checks 33814
ENABLED FireEye Compliance Checks 70469
ENABLED HP ProCurve Compliance Che... 70271
ENABLED IBM iSeries Compliance Checks 57860
Save
Cancel

Editing a Scanning Policy to see if Policy Compliance is available

To enable use of an `.audit` file, under the "**Preferences**" tab select "Cisco IOS Compliance Checks", "Huawei Compliance Checks", "Unix Compliance Checks", "Windows Compliance Checks", "Windows File Content Compliance Checks", "IBM iSeries Compliance Checks", or "Database Compliance Checks" from the drop-down menu. There will be five fields in each

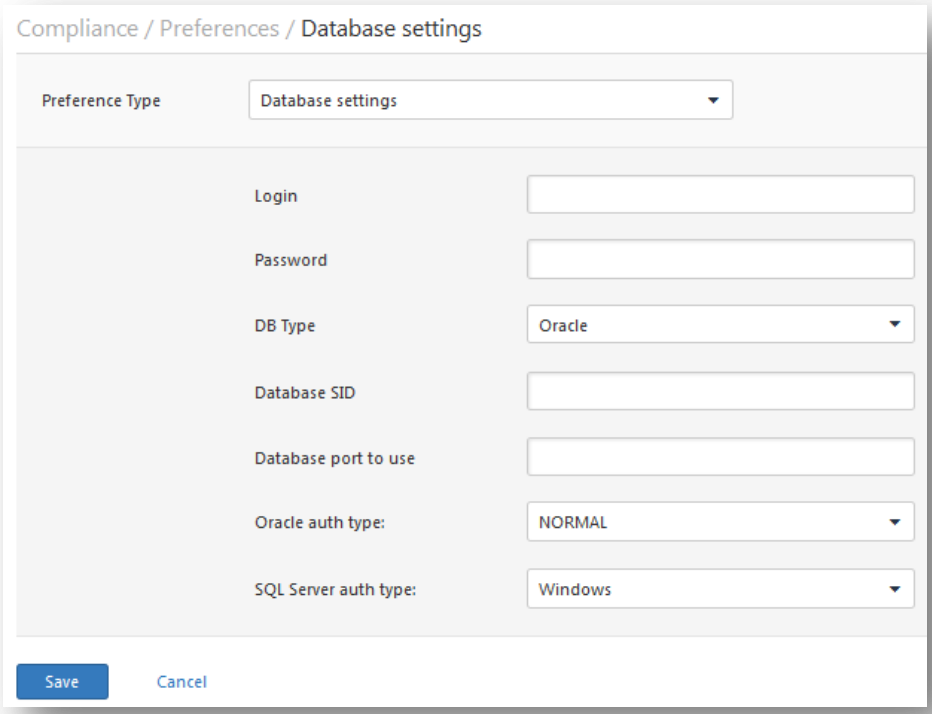
Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

section that can specify separate `.audit` files. The files specified will have been previously downloaded to the local client system from the Tenable Support Portal.



Example Nessus User Interface dialog box to specify Unix .audit files

If "Database Compliance Checks" was selected in the previous drop-down menu, login parameters for the database must be entered under "**Preferences**" -> "**Database Settings**":



Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

A number of options under “Database Settings” are available including:

Option	Description
Login	The username for the database.
Password	The password for the supplied username.
DB Type	Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and PostgreSQL are supported.
Database SID	Database system ID to audit. Applicable to Oracle, DB2, and Informix only.
Oracle auth type	NORMAL, SYSOPER, and SYSDBA are supported.
SQL Server auth type	Windows or SQL Server are supported.

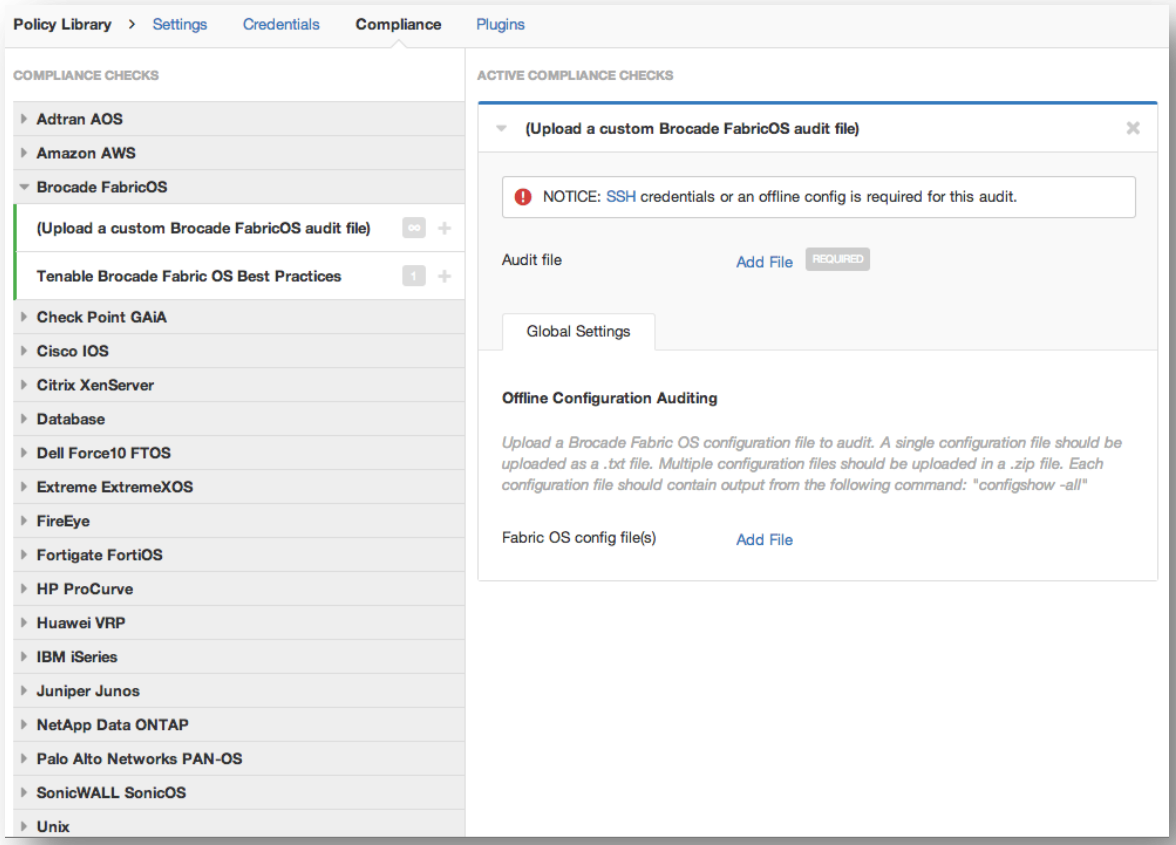
Consult with your local database administrator to obtain the correct values for these fields.

At this point, click on “Save” at the bottom of the window and the configuration will be complete. The new scan policy will be added to the list of managed scan policies.

Uploading a Custom Audit Policy

In addition to using pre-defined audit policies that Tenable provides, users can create their own custom audit policies. In order to use them in the policy, you must upload the policy under the appropriate compliance check section.

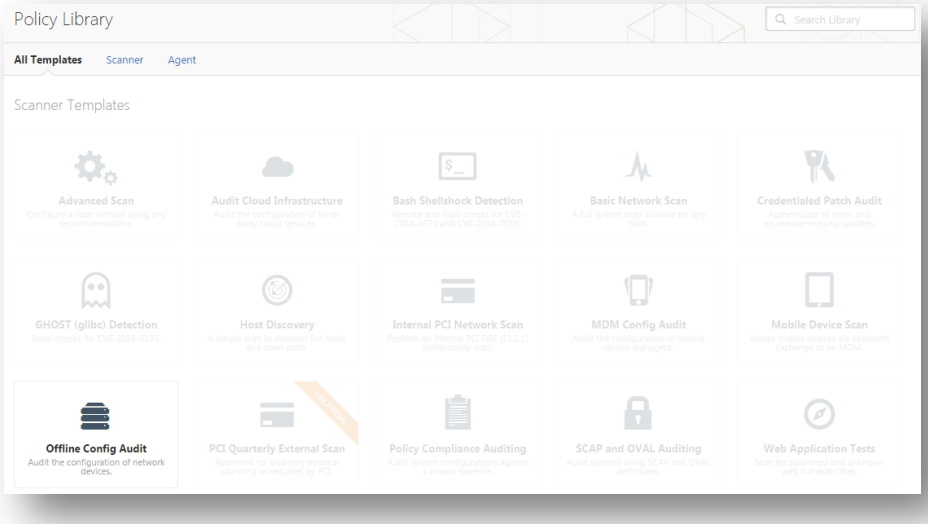
Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.



Offline Configuration Audits

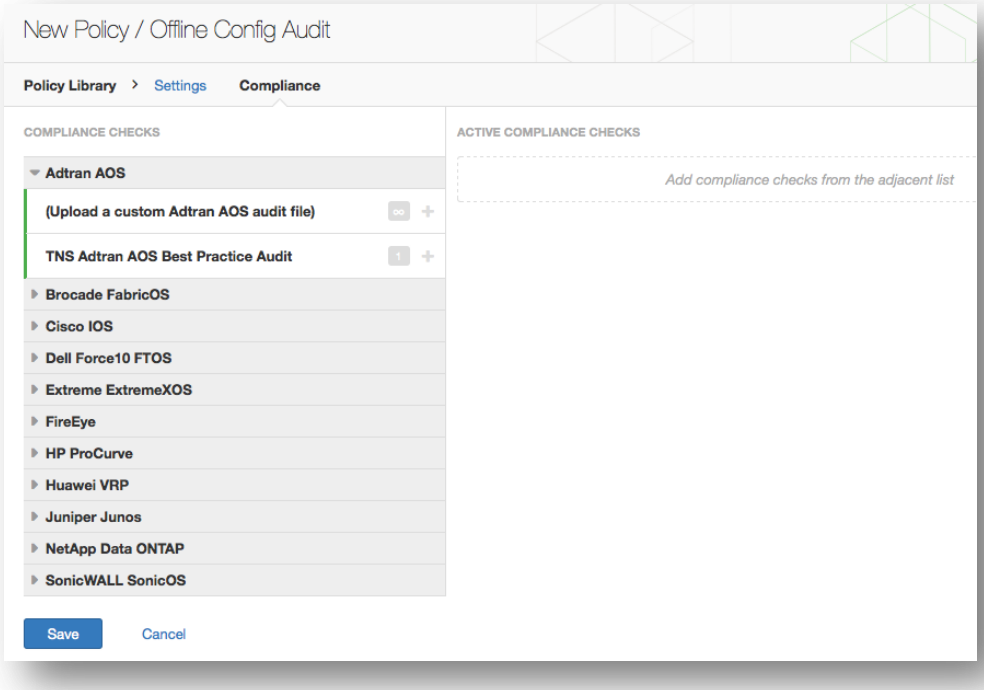
For sensitive devices that cannot afford downtime, Tenable offers offline configuration audits. This requires the user to upload the configuration file to the Nessus policy.

To create an offline configuration audit, select the **Offline Config Audit** in the new Policies library:

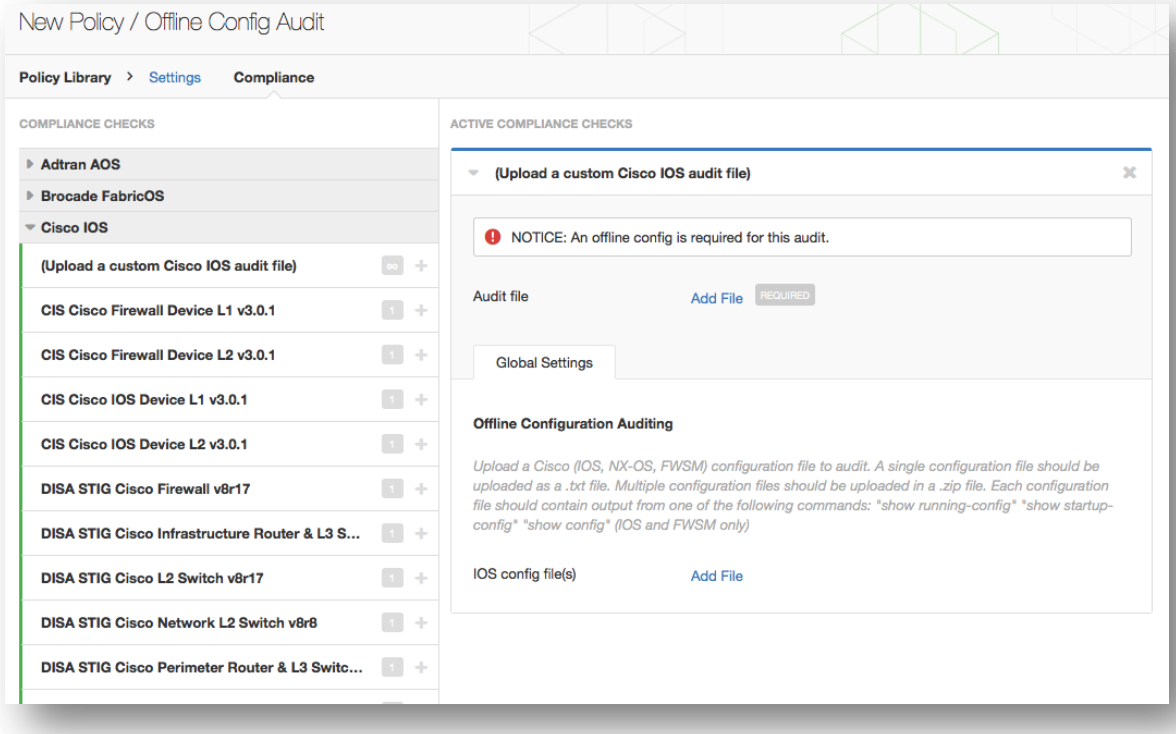


Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

To see the compliance options, click on the **Compliance** menu. This will bring up options different than the standard compliance audit. The left column shows the supported network devices that can have their configurations audited offline:



For each device, an audit policy and a configuration file are required. Audits can either be custom or a pre-defined audit available through the Nessus policy:


New Policy / Offline Config Audit
Policy Library
Settings
Compliance
COMPLIANCE CHECKS
ACTIVE COMPLIANCE CHECKS
Adtran AOS
Brocade FabricOS
Cisco IOS
(Upload a custom Cisco IOS audit file)
CIS Cisco Firewall Device L1 v3.0.1
CIS Cisco Firewall Device L2 v3.0.1
CIS Cisco IOS Device L1 v3.0.1
CIS Cisco IOS Device L2 v3.0.1
DISA STIG Cisco Firewall v8r17
DISA STIG Cisco Infrastructure Router & L3 S...
DISA STIG Cisco L2 Switch v8r17
DISA STIG Cisco Network L2 Switch v8r8
DISA STIG Cisco Perimeter Router & L3 Switc...
(Upload a custom Cisco IOS audit file)
NOTICE: An offline config is required for this audit.
Audit file
Add File
REQUIRED
Global Settings
Offline Configuration Auditing
Upload a Cisco (IOS, NX-OS, FWSM) configuration file to audit. A single configuration file should be uploaded as a .txt file. Multiple configuration files should be uploaded in a .zip file. Each configuration file should contain output from one of the following commands: "show running-config" "show startup-config" "show config" (IOS and FWSM only)
IOS config file(s)
Add File

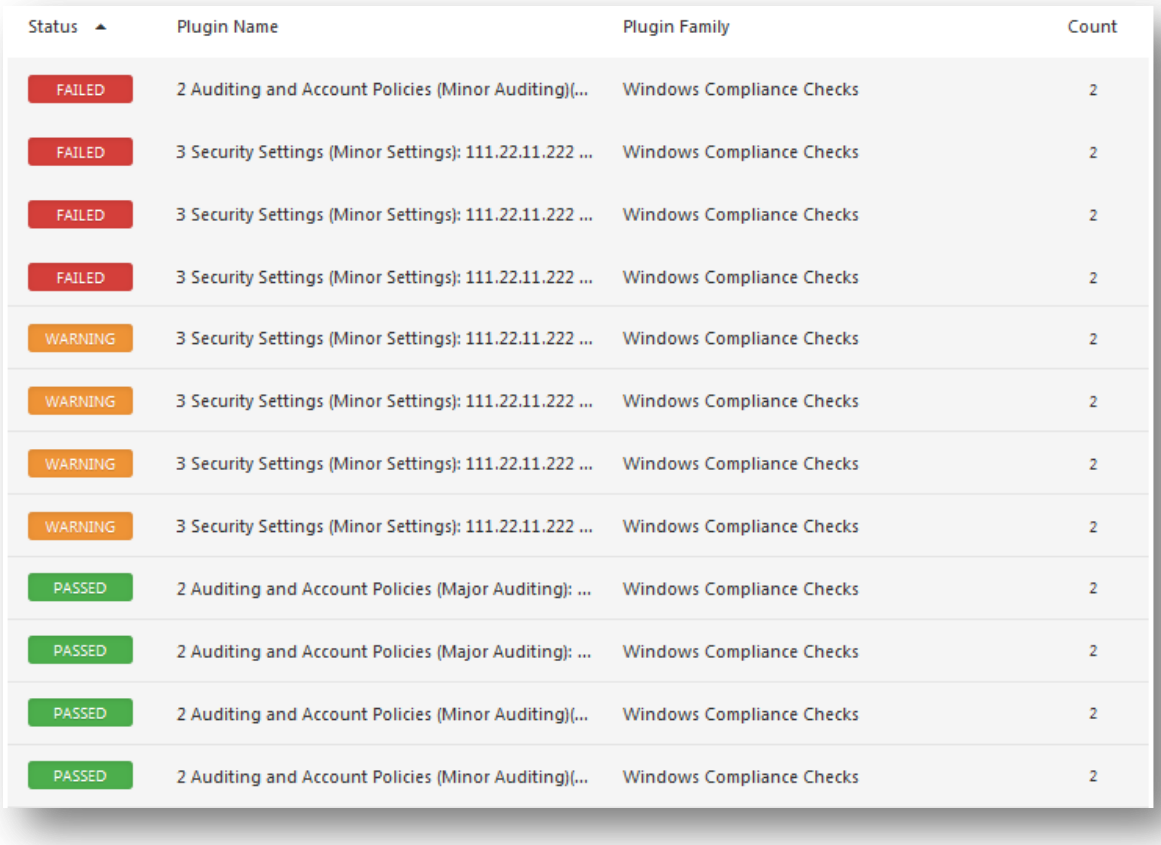
Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Performing a Scan

Running a scan that has compliance checks enabled is no different than running other local patch auditing scans or even regular network scans. In fact, these can be mixed and matched to all run at the same time, if desired.

Example Results

In Nessus, all compliance results are returned with the plugin ID performing the test. In the example below, all data that is returned for a scanned Windows server will be from the Windows Compliance `.nbin` plugin, identified as plugin 21156.



Status	Plugin Name	Plugin Family	Count
FAILED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Major Auditing): ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Major Auditing): ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2

Example Compliance Results while scanning a Windows Server

The HTML report, which can be downloaded from the "Reports" tab in the Nessus user interface, highlights compliance tests that pass with blue and a "PASSED" message; those that fail with red and a "FAILED" message; and any items that could not be audited are highlighted with yellow and an "WARNING" message.

In the above example, only four items are shown. Each of these items was from an access control policy checking for the presence of unnecessary and insecure services and protocols. Some of these services were not running and met the expectations of the `.audit` policy, while others (such as the "remote registry" service) were running and were listed as "FAILED". It is strongly recommended that items listed as "FAILED" be configured to meet the policy as according to your security standards.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Example Nessus for Unix Command Line Usage

Obtaining the Compliance Checks

If your commercial Nessus installation has been configured, there will be five compliance **.nbin** files in your plugins directory.

Obtain any needed **.audit** files from the Tenable Support Portal located at https://support.tenable.com/, and place them in your scanner's plugins directory. On most distributions, the default location is the following directory:

/opt/nessus/lib/nessus/plugins

These plugins will be present among the more than 40,000 **.nasl** plugin files used by Nessus for performing vulnerability scanning. You can search for these by looking for the **.nbin** extension as shown below:

```
# ls compliance*nbin

cisco_compliance_check.nbin                 database_compliance_check.nbin
compliance check.nbin                       unix compliance check.nbin
compliance_check_windows_file_content.nbin  …
```

There may be other **.nbin** files delivered by Tenable, such as the Skype plugin, that have nothing to do with performing compliance checks.

If you do not have local access to the actual Nessus daemon, but do have a username and password to log in to the server, you can request a list of plugins by using the "**-p**" option of the **nessus** command line client as shown below:

```
# /opt/nessus/bin/nessus -xp 192.168.20.1 1241 username password | grep 21156
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
21156|Policy Compliance|Checks if the remote system is compliant with the
      policy|infos|This script is Copyright (C) 2006 Tenable Network Security|Check
      compliance policy|$Revision: 1.3 $|NOCVE|NOBID|NOXREF|\nSynopsis :\n\n
      Compliance checks\n\nDescription :\n\nUsing the supplied credentials this
      script perform a compliance\ncheck against the given policy.\n\nRisk factor
      :\n\nNone
```

The query may take a few minutes to run. If your query runs successfully but does not return any data, then the compliance checks are not installed on the remote Nessus scanner.

Using .nessus Files

Nessus has the ability to save configured scan policies, network targets, and reports as a **.nessus** file. The section "Example Nessus User Interface Usage" describes creating a **.nessus** file that contains a scanning policy for compliance checks. For instructions on running a command line scan using the **.nessus** file, refer to the "Nessus User Guide" available at: http://www.tenable.com/products/nessus/documentation.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Using .nessusrc Files

To invoke a command line scan with Nessus, you need to specify the following:

- The Unix, Windows, or database compliance check plugins
- Credentials for the target host(s) being scanned
- One or more **.audit** files for the compliance check plugins to run
- That dependencies have been enabled

Relevant entries in a **.nessusrc** file have the following format (with some content omitted):

```
begin(SERVER_PREFS)
…
auto_enable_dependencies = yes
…
end(SERVER_PREFS)
begin(PLUGINS_PREFS)
…
Compliance policy file(s) : = federal_nsa_microsoft_xp_file_permissions.audit
…
end(PLUGINS_PREFS)
begin(PLUGIN_SET)
 21156 = yes
 21157 = yes
…
End(PLUGIN_SET)
```

The previous example has left out many other pieces of data that specify what a scan can perform. The omitted content includes enabling the specific **.audit** policy file in use, enabling dependencies, and the actual compliance plugins themselves.

Performing a Scan

Running a scan that has compliance checks enabled is no different than running other local patch auditing scans or even regular network scans. In fact, these can be mixed and matched to all be run at the same time, if desired.

Example Results

As with the GUI clients, all detected compliant or non-compliant results are reported in the following format:

```
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Reset lockout account counter
      after" : [FAILED]\n\nRemote value: 30\nPolicy value: 20\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password length" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 8\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password age" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 1\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Maximum password age" :
      [FAILED]\n\nRemote value: 42\nPolicy value: 182\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Enforce password history" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 5\n\n\n
```

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

```
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout threshold" :
      [FAILED]\n\nRemote value: 0\nPolicy value: 3\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout duration" :
      [FAILED]\n\nRemote value: 30\nPolicy value: 60\n\n\n
```

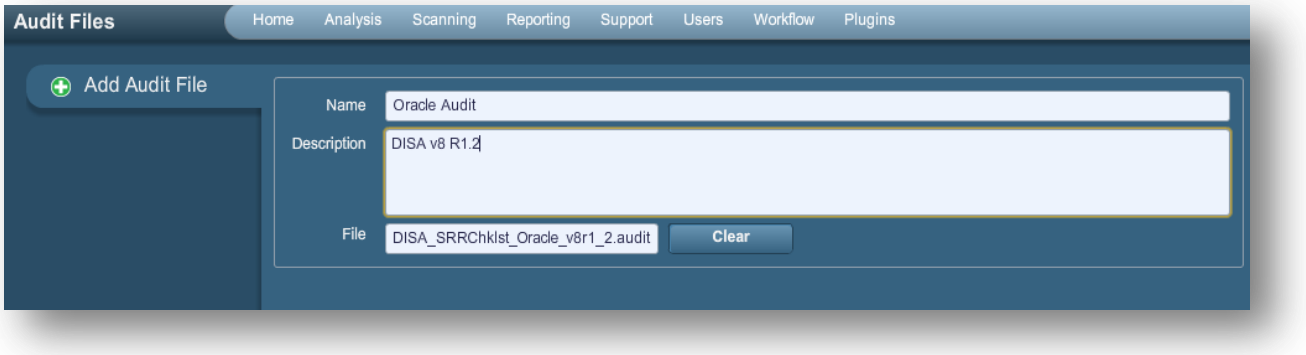
This data is in the **.nsr** report format for Nessus. These are all non-compliant events.

SecurityCenter Usage

The information below is based on running compliance scans with SecurityCenter 4 or greater. For Security Center 3.x users, please refer to the "Security Center 3.4 Documentation" available on the Tenable Support Portal: https://support.tenable.com/.

Obtaining the Compliance Checks

All SecurityCenter customers have access to the Nessus commercial plugins. This includes the Cisco, IBM iSeries, Unix, Windows, Windows File Contents, and Database compliance check plugins. These plugins allow the user to upload and run compliance scans using prebuilt and customizable **.audit** files provided by Tenable. Obtain any of the required **.audit** files from the Tenable Support Portal located at https://support.tenable.com/. These **.audit** files can be uploaded to SecurityCenter by any user with the "Create Audit Files" permission by using the "Add Audit File" tool within the "Support" tab.

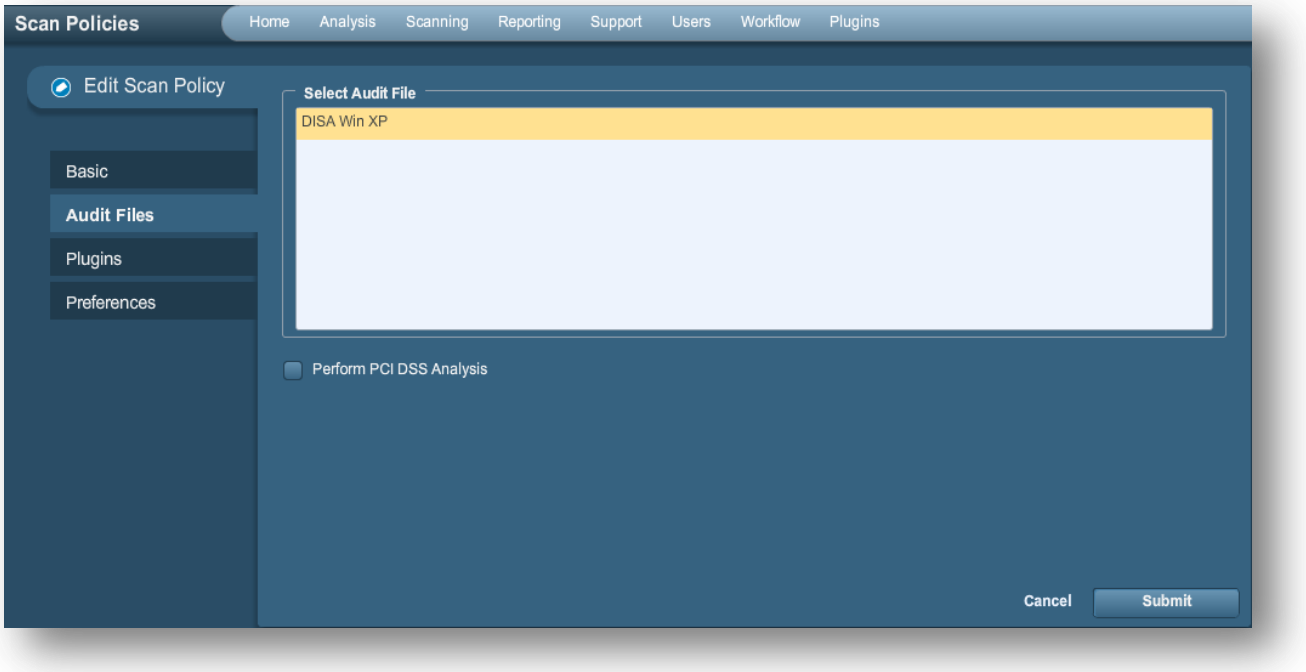


Any **.audit** files uploaded to SecurityCenter will be available for any SecurityCenter user with the "Create Policies" permission. SecurityCenter will also handle distributing new and updated **.audit** files to the Nessus scanners.

Configuring a Scan Policy to Perform a Compliance Audit

To perform a compliance scan with SecurityCenter, users must configure a scan policy with the appropriate compliance-related settings. This policy specifies the scan options, audit files, enabled plugins, and advanced preferences. The second page of the "Scan Policy" specifies the **.audit** files to be used for the compliance audit.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.



Here, one or more `.audit` files can be selected by highlighting the `.audit` file and clicking on "Submit". For selecting multiple `.audit` files, use the "Ctrl" key to perform multi-select. If a basic PCI DSS analysis is required, ensure that the "Perform PCI DSS Analysis" checkbox is selected before submitting.

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, American Express, Discover Financial Services, and MasterCard. The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is in use by many e-commerce vendors who accept and store credit card data.

Tenable provides twelve plugins to all SecurityCenter users that automate the process of performing a PCI DSS audit. For the list of plugins, see the table below.

These plugins evaluate the results of your scan and the actual configuration of your scan to determine if the target server meets published PCI compliance requirements. The plugins do not perform actual scanning; instead, they look at the results from other plugins. To activate the PCI DSS plugins, simply check the box labeled "Perform PCI DSS Analysis" from the "Compliance" screen.

After selecting the desired `.audit` file(s) and PCI DSS settings, click on the "Plugins" tab to confirm plugin settings. Items within the plugin family "Policy Compliance" must be enabled in the policy to perform a compliance scan.

When the user selects one or more audit files under the "Audit Files" tab of the scan policy, the correct plugin is automatically enabled under the "Plugins" tab. SecurityCenter analyzes the selected `.audit` file(s) and based on the type specified within the file, the correct plugin(s) are enabled.

Under the "Policy Compliance" family are fourteen plugins available for compliance auditing. These include the following:

Plugin ID	Plugin Name	Plugin Description
21156	Windows Compliance Checks	Used to audit common Windows configuration settings.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

21157	Unix Compliance Checks	Used to audit common Unix configuration settings.
24760	Windows File Contents Compliance Checks	Used to audit sensitive file contents on Windows servers.
33814	Database Compliance Checks	Used to audit common database configuration settings.
33929	PCI DSS compliance	Determine if the remote web server is vulnerable to cross-site scripting (XSS) attacks, implements old SSL2.0 cryptography, runs obsolete software, or is affected by dangerous vulnerabilities (CVSS base score >= 4).
57581	PCI DSS Compliance: Database Reachable from the Internet	Detects the presence of a database reachable from the Internet, resulting in a failed compliance audit.
60020	PCI DSS Compliance: Handling False Positives	Notes the proper handling of false positives in PCI DSS scans.
56208	PCI DSS Compliance: Insecure Communication Has Been Detected	Determines if an insecure port, protocol, or service has been detected, that would result in failing compliance.
56209	PCI DSS Compliance: Remote Access Software Has Been Detected	Detects the presence of remote access software that would result in failing compliance.
33930	PCI DSS Compliance: Passed	Using the available scan information, Nessus did not find any disqualifying flaws for this host.
33931	PCI DSS Compliance: Tests Requirements	Analyze whether the Nessus scan meets PCI test requirements or not. Even if the technical tests passed, this report may be insufficient to certify this server.
46689	Cisco IOS Compliance Checks	Used to audit common Cisco device configuration settings.
73157	Huawei Compliance Checks	Used to audit common Huawei device configuration settings.
57860	IBM iSeries Compliance Checks	Used to audit common IBM iSeries configuration settings.

Managing Credentials

One advantage of SecurityCenter in performing credentialed-based scans is that it can help manage the credentials in use. Credentials are created in SecurityCenter by selecting the “Support” tab, clicking on “Credentials”, and then clicking on “Add”.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Unix, Windows, Cisco, and database credentials are stored and managed separate from the scan policy. Credentials can be created with “User” visibility for the current user or “Organizational” visibility where they can be used by other SecurityCenter users. This allows users to work with the results of the scans and perform new scans without actually needing to know the credentials involved with the scanning.

Analyzing the Results

SecurityCenter can be used to analyze and report on compliance data returned by the Nessus scans in many ways. Common reports include:

- Listing of all compliant or non-compliant vulnerabilities by asset group
- Listing of all compliant or non-compliant vulnerabilities by host or network
- Summary of all non-compliant issues
- Auditing database settings for common misconfigurations
- Reporting user or software status based upon IT needs

Once the compliance data has been discovered by SecurityCenter, the ticketing, reporting, and analytical tools can be used to determine the best course of action for re-configuring the audited devices. This data can be analyzed in parallel with other vulnerability, security patch or passively discovered information.

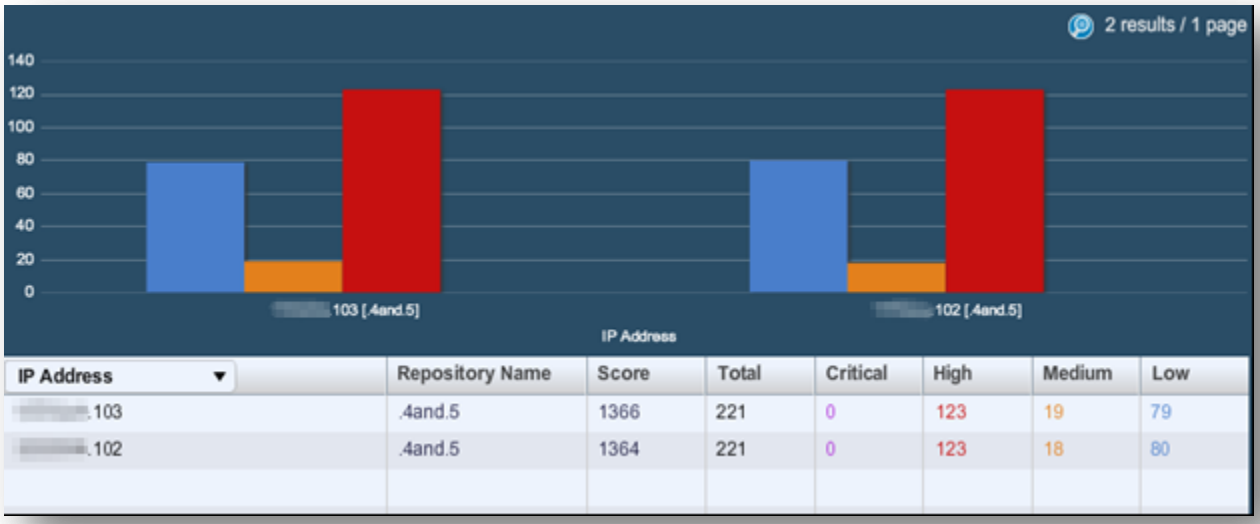
Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

Some example screen captures of SecurityCenter being used to analyze compliance information about scanned hosts are shown below:

Plugin ID	Total ▼	Severity	Name
1000282	4	Low	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\allocatedasd
1000295	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlog\\AutoAdminLogon
1000294	4	Low	HKLM\\System\\CurrentControlSet\\Control\\SecurePipeServers\\Winreg\\AllowedPaths\\Machine
1000293	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionPipes
1000292	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionShares
1000291	4	Medium	HKLM\\Software\\Policies\\Microsoft\\Cryptography\\ForceKeyProtection
1000290	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\ForceGuest
1000289	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\LimitBlankPasswordUse
1000288	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinClientSec
1000287	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinServerSec
1000286	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\NoDefaultAdminOwner
1000285	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LDAP\\LDAPClientIntegrity
1000284	4	Low	HKLM\\Software\\Microsoft\\Driver Signing\\Policy
1000283	4	High	HKLM\\software\\microsoft\\non-driver signing\\policy
1000296	4	Low	HKLM\\System\\CurrentControlSet\\Control\\FileSystem\\NtfsDisable8dot3NameCreation
1000281	4	High	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\scremoveoption
1000280	4	High	HKLM\\system\\currentcontrolset\\control\\lsa\\lmcompatibilitylevel
1000279	4	High	HKLM\\system\\currentcontrolset\\control\\print\\providers\\lanman print services\\servers\\addprinterdrive
1000278	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\AutoAdminLogon
1000277	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkNoDialIn
1000276	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkHideSharePwds
1000275	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDriveTypeAutoRun
1000274	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\PerformRouterDiscovery
1000273	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\SynAttackProtect
1000272	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\DisableIPSourceRouting
1000271	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\KeepAliveTime
1000270	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableDeadGWDetect
1000269	4	High	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableICMPRedirect

Example listing of Compliance Audit Data with SecurityCenter

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.



IP Address	Repository Name	Score	Total	Critical	High	Medium	Low
.103	.4and.5	1366	221	0	123	19	79
.102	.4and.5	1364	221	0	123	18	80

Example listing of Compliance Audit Data by Server with SecurityCenter

For more information about using SecurityCenter, please refer to the SecurityCenter documentation available at https://support.tenable.com/.

Additional Resources

Tenable has produced a variety of other documents detailing Nessus' installation, deployment, configuration, user operation, and overall testing:

- Nessus 6.4 Installation and Configuration Guide – step by step walk through of installation and configuration for Nessus Professional, Nessus Manager, Nessus Cloud, and Nessus Agents
- Nessus 6.4 User Guide – how to configure and operate the Nessus User Interface for Nessus Professional, Nessus Manager, Nessus Cloud, and Nessus Agents
- Nessus 6.4 Command Line Reference – describes the Nessus command line tools for Nessus Professional, Nessus Manager, and Nessus Agents
- Nessus v6 SCAP Assessments – describes how to use Tenable's Nessus to generate SCAP content audits as well as view and export the scan results
- Nessus Compliance Checks – high-level guide to understanding and running compliance checks using Nessus and SecurityCenter
- Nessus Compliance Checks Reference – comprehensive guide to Nessus Compliance Check syntax
- Nessus v2 File Format – describes the structure for the `.nessus` file format, which was introduced with Nessus 3.2 and NessusClient 3.2
- Nessus and Antivirus – outlines how several popular security software packages interact with Nessus, and provides tips or workarounds to allow the software to better co-exist without compromising your security or hindering your vulnerability scanning efforts

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.

- Comprehensive Malware Detection with SecurityCenter Continuous View and Nessus – describes how Tenable's SecurityCenter CV can detect a variety of malicious software and identify and determine the extent of malware infections
- Real-Time Compliance Monitoring – outlines how Tenable's solutions can be used to assist in meeting many different types of government and financial regulations
- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner
- SecurityCenter Administration Guide

Other online resources are listed below:

- Nessus Discussions Forum: https://discussions.nessus.org/
- Tenable Blog: http://www.tenable.com/blog
- Tenable Podcast: http://www.tenable.com/podcast
- Example Use Videos: http://www.youtube.com/user/tenablesecurity
- Tenable Twitter Feed: http://twitter.com/tenablesecurity

Please feel free to contact Tenable at support@tenable.com, sales@tenable.com, or visit our web site at http://www.tenable.com/.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.

Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.